

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

Appl. No. : 09/823,833  
Filed : March 30, 2001

35. The method in accordance with Claim 31 wherein said resetting comprises providing power to said peripheral device.

36. The method in accordance with ~~Claim 31~~ wherein said authenticating step comprises generating a signature from said new control code and comparing said signature to a signature provided with said new control code.

REMARKS

This is in response to the Office Action mailed July 17, 2002. By this Response, Applicants have canceled Claim 5, have amended Claims 1-3, 6 and 9, and have added new Claims 31-36. Claims 1-4 and 6-36 are now pending in the application after this Response.

By the Office Action, the Examiner indicated the rejection of Claims 1, 2, 5, 9, 23, and 25 under 35 U.S.C. § 112 as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. The Examiner also indicated rejection of Claims 1, 4, 7-17, 19, 23-27, and 30 under 35 U.S.C. § 102 as being anticipated by Acres et al. (# 5,702,304). Further, Examiner indicates rejection of Claims 2-3, 5-6, and 29 under 35 U.S.C. § 103 as being unpatentable over Acres and Claims 18, 20-22, 28 as being unpatentable over Acres in view or McCauley (# 6,263,392).

**Appl. No.** : 09/823,833  
**Filed** : March 30, 2001

REMARKS FOR CLAIM REJECTIONS - 35 U.S.C. § 112

Independent Claim 1

Applicants have amended Claim 1 and assert that the claim complies with Section 112.

Dependent Claims 2, 5

Applicants have canceled Claim 5 to eliminate its redundancy with Claim 2.

Independent Claim 9

Applicants have amended Claim 9 to recite that the peripheral device provides a signal for causing control code to be transmitted from a remote location to said peripheral and believe that Claim 9 complies with Section 112(2).

Dependent Claim 23

The Examiner indicates that “identification of the peripheral device would have to be a known element before sending the code.” As indicated in the specification (see page 20, line 20 to page 22, line 5) in accordance with an invention, upon the gaming controlling receiving a signal from a peripheral designating the existence of the peripheral, the gaming controller downloads code to the peripheral. The peripheral then executes the code to configure itself. The peripheral can then transmit a signal to the gaming controller which identifies the peripheral as a particular peripheral device, such as a bill validator or coin acceptor. Claim 23 is directed to this aspect of the invention.

Independent Claim 25

Applicants have amended Claim 25 to more particularly claim the invention and believe that Claim 25 complies with Section 112(2).

**Appl. No.** : 09/823,833  
**Filed** : March 30, 2001

**REMARKS REGARDING CLAIM REJECTIONS - 35 U.S.C. §§ 102/103**

**The Present Invention Is Fundamentally Different Than That Disclosed in Acres**

The Examiner's rejections of the pending claims are all based upon U.S. Patent No. 6,702,304 to Acres. Applicants assert that the invention disclosed in Acres is fundamentally different from the invention claimed in the present application.

Applicants' invention is a method by which executable control code is provided to peripheral to enable operation of the peripheral device. In some instances, a peripheral device may have no operating code, and thus operating code must be provided. This may occur, for example, when the gaming machine is first being placed into operation. In another instances, the operating code may be obsolete or corrupt and require replacement.

As described in the specification of the present application, for example, during the continued operation of the gaming device, it may be determined that the code of the bill validator peripheral device must be changed, such as to accommodate a change in currency format (such as a new bill design introduced by the US Treasury). In accordance with an embodiment of the invention, updated operating code can be provided to the peripheral device to provide this functionality.

Contrary to the present invention, Acres does not disclose a method or system for providing code to a peripheral device of a gaming machine. Instead, Acres discloses an environment where a gaming machine is pre-loaded with a fixed set of code and that code does not change. Acres simply discloses sending a "reconfiguration command" from a data communication node (DCN) to the gaming machine. This reconfiguration command is simply an instruction to the gaming machine

**Appl. No.** : 09/823,833  
**Filed** : March 30, 2001

to invoke a different function or property of the already existing code and does not involve transmitting any new code.

Once this fundamental difference between the present invention and the invention described in Acres is understood, other differences between the inventions will be apparent. For example, in accordance with one embodiment of Applicants' invention, a peripheral device signals the gaming controller of the peripheral device's existence, causing the gaming controller to provide code to the peripheral which the peripheral can execute to operate.

In comparison, Acres recites a method of polling a gaming machine to "determine its level of activity"(23:50-51). "In response, the machine will send a packet of status information indicating the current amount of activity on the machine. The status information included in the response will depend on the type of machine that the DCN is in communication with" (23:53-57). Thus, in Acres a remote DCN sends a polling signal to a gaming machine, as opposed to a peripheral device sending a signal to a gaming controller.

Applicants' invention also includes a variety of other features, including the authentication of code. As detailed in the Background portion of the present application, one problem with gaming machines is that people may attempt to tamper with the code. As indicated, Acres does not disclose providing new executable code to a device, but simply invoking a new operation or feature of that device which already exists. Thus, the existing code may be tampered with. The present invention overcomes the problem with systems such as that disclosed in Acres because control code for a peripheral may be re-loaded upon the occurrence of any of a variety of events, such as a reboot or

**Appl. No.** : 09/823,833  
**Filed** : March 30, 2001

a power failure. When re-loaded, the code is authenticated, ensuring that the peripheral is only operating authenticated control code.

Applicants assert that the Examiner has taken the Acres disclosure out of context and further assert that, when what Acres actually discloses is compared carefully to the language of the claims of the application, it is clear that the claims define patentable subject matter over Acres.

#### Discussion Regarding Each Claim

##### Independent Claim 1

Independent Claim 1 recites a method of operating a game device having a controller with at least one peripheral device. In accordance with the method, a peripheral device provides a signal to the game device controller, causing the game device controller to provide executable control code to the peripheral device.

As discussed above, there are fundamental differences between this method and that disclosed in Acres. First, Acres does not teach a method involving a gaming device controller and a peripheral device of a gaming device. Acres does not disclose a method involving a gaming device peripheral at all, but only a system including a gaming device and a remote DCN.

Second, Acres does not teach or disclose the step of transmitting a signal from a peripheral device to a gaming device controller. Acres discloses transmitting a reconfiguration command from a remote DCN to a gaming machine. In particular, Acres discloses that a DCN controller “transmits reconfiguration commands to the gaming device in order to reconfigure the payout schedule of the machine in accordance with the reconfiguration command.(23:1-6)”. In addition, as indicated in the

**Appl. No.** : 09/823,833  
**Filed** : March 30, 2001

System Overview of the Description of Acres (6:35-39), “the gaming devices, on receiving a reconfiguration command, will reconfigure its jackpot payout schedule in accordance with the reconfiguration command.”

Acres also does not disclose a method where, in response to the signal transmitted from a peripheral device to a controller of a gaming device, control code is transmitted to the peripheral device, and that same transmitted code is stored and then executed.

In Acres, no code is transmitted to a peripheral device. As indicated, at most a reconfiguration command is transmitted, the command invoking a particular function or feature at the gaming machine which already exists. In Acres, code already exists at the gaming machine and the reconfiguration command simply invokes a particular action or activity already programmed into that code. No new code is transmitted, stored and then executed.

#### Independent Claim 9

Independent Claim 9 recites a method of providing control code to enable operation of a peripheral device associated with a gaming device controller. Once again, Applicants assert that Acres does not disclose a system or method involving a gaming device having a gaming device controller and associated peripherals, but a system where a remote DCN sends reconfiguration commands to a gaming machine.

Thus, Acres does not teach providing a peripheral controller, providing a signal which causes control code to be delivered to a peripheral device, or storing and executing the code received in response to the signal.

**Appl. No.** : 09/823,833  
**Filed** : March 30, 2001

Independent Claim 25

Independent Claim 25 recites a gaming device having a controller and at least one peripheral having a controller with resident code. The resident code of the peripheral controller is adapted to cause the peripheral controller to obtain control code for controlling the peripheral device. The peripheral also includes data storage for storing code which is transmitted in response to a signal provided to the gaming device controller.

Once again, Applicants assert that Acres does not disclose a gaming device having a controller, as well as a peripheral having a controller. Acres also does not disclose a peripheral having a controller with resident code which is configured to obtain control code for the peripheral, or a system where control code is transmitted and stored in response to a signal provided to a gaming control device. Acres discloses only transmitting a reconfiguration signal from a remote DCN to a gaming machine, the signal invoking a function or feature already existing at the gaming machine. Acres does not disclose transmitting control code to effect operation of a peripheral.

Dependent Claims

Claims 2-4 and 6-8

Claims 2-4 and 6-8 are believed to be allowable for at least the reason that they depend from allowable independent Claim 1.

Claims 2-3 and 6 disclose a method of initiating, resetting, and removing data from a programmable memory stored in a peripheral device. Acres does not teach any method comprising the use of a peripheral device or a memory associated with such a peripheral device. Acres

**Appl. No.** : 09/823,833  
**Filed** : March 30, 2001

discusses a power up procedure related to initialization of a random access memory associated with a data communication node (DCN) and not a peripheral device (21:20-30).

The portion of Acres to which the Examiner refers (7:16-25) does not teach or disclose any sort of peripheral device within a gaming machine. As shown in Figure 1 of Acres, the game devices that are referenced as elements 12-16 (7:17-18) are analogous to game devices such as that representing a slot machine. A peripheral device is a subset or component of the game device that communicates to a game controller. In comparison, the game device Acres discloses is analogous to the game device Applicants refer to as element 20 in Figures 1 and 2 of the present application.

Applicants also assert, contrary to the Examiner's contention, that the mere act of providing power does not necessitate resetting a programmable memory, as there are programmable memories that are non-volatile, having an embedded power source such as a battery that allows them to continue to maintain data and to continue operation.

Specifically, with respect to Claims 2 and 6, Applicants assert that Acres in no way teaches or suggests transmitting a signal from a peripheral device to a gaming device controller in response to the providing of power to a peripheral, and where the signal causes control code to be provided to the peripheral.

With respect to Claim 3, Applicants similarly assert that Acres in no way teaches or suggests transmitting a signal from a peripheral device to a gaming device controller in response to the resetting of the peripheral device, and where the signal causes control code to be provided to the peripheral.

**Appl. No.** : 09/823,833  
**Filed** : March 30, 2001

With respect to Claim 7, Applicants claim a method of sending a digital signature as a method of authenticating executable control code transmitted to a peripheral device of a gaming machine. This is quite distinct from using a “CRC” protocol on a reconfiguration command as disclosed in Acres. Applicants assert that these algorithms differ both in function and in use. Utilizing a digital signature provides a more sophisticated method of authenticating data as performed on executable code or software application programs. A CRC (cyclic redundancy check) is typically performed during transmission of data packets from one location to another as when a CRC is performed at layer 2 of the OSI model during packet data transmission or in the adaptation layer of an ATM transmission.

Applicants’ method, unlike CRC, is authentication which ensures that the control code which is transmitted to a peripheral is not corrupt or has not been tampered with. Applicants contend that using a digital signature approach provides an additional feature in that it provides an indication that an application file may have been modified in addition to the accuracy of bits sent from one location to another. If changes are made to the file, then the signature will change. In this way, the signature of a file can be used as a quick verification to see if anyone has altered the file, or if it has lost a bit during transmission. Applicants assert that Acres only indicates the transmission of a “data packet” that includes a CRC frame (23:15-18). Acres does not disclose the use of a digital signature to verify alteration of critical data.

**Appl. No.** : 09/823,833  
**Filed** : March 30, 2001

Claims 10-24

Claims 10-24 are believed allowable for at least the reason they depend from allowable independent Claim 9.

Claims 10-12 and 19 are believed allowable as they claim a method of authenticating a control code prior to being sent from a gaming controller and after it is received at a peripheral device. Acres does not disclose any form of authentication. This is because Acres does not disclose the transmission of executable control code. Authentication of such control code is performed in accordance with the Applicants' invention to ensure reliable operation of a gaming machine's peripherals. Acres also does not disclose any type of authentication utilizing hashing operations and signatures before data is transmitted. Acres merely discusses how a CRC algorithm can be used to transmit data provided by data packets.

Claim 13 is believed allowable for similar reasons to Claim 7 discussed above. As explained above, Acres does not disclose authenticating data, but only using a CRC algorithm to provide a check on the transmission of packets (23:15-18).

Claim 14 recites a method of providing control code used to operate a peripheral device by transmitting code from a remote device by a way of a gaming device controller. Acres does not disclose a method of providing control code; rather, Acres discloses a method of modifying operation by sending a reconfiguration command to the gaming device (23:24-25).

Claim 15 recites a method of providing control code in which a transmitted signal which causes the transmission of the code to a gaming device peripheral is a signal designating the peripheral device as a download device. Acres does not disclose transmitting control code to a

**Appl. No.** : 09/823,833  
**Filed** : March 30, 2001

peripheral device of a gaming machine. As such, Acres further does not disclose transmitting a signal which designates a peripheral device as a download device in order to cause the code to be transmitted.

Claim 16 is believed allowable as it recites a method whereby resident code residing in a memory of a peripheral device is executed to allow another version of control code to be downloaded. Acres does not disclose any resident code residing in a peripheral device within a gaming machine causing a generation of any signal. Instead, Acres describes a method of eliciting a “status message from the DCN to the machine over the serial machine interface. In response, the machine will send a packet of status information indicating the current amount of activity on the machine.”(23: 58-67)

Claims 17 and 18 are believed allowable as they recite a method where code is transmitted to a peripheral in response to a signal from a gaming device controller. As claimed in Claim 18, the controller is a USB device. Acres does not disclose transmitting a signal which causes code to be transmitted to a peripheral device, let alone a configuration where a gaming device controller is configured as a USB device.

Claims 20-22 discloses methods of verifying executable control code transmitted to a peripheral for execution. Neither Acres or McCauley discloses any form of authentication similar to that disclosed by the Applicants either before or after data is sent to a peripheral device because executable control code is not verified. Authentication of such control code is performed by the Applicants’ invention to insure reliable operation of a gaming machine’s peripherals. Further, Acres nor McCauley discloses any type of authentication utilizing hashing operations and signatures before

**Appl. No.** : 09/823,833  
**Filed** : March 30, 2001

data is transmitted. Acres merely discusses how a CRC algorithm can be used to transmit data provided by data packets. Examiner references McCauley (7:29-47); however, this reference provides no indication of a verification of control codes in any form or fashion. As a consequence, these claims are believed to define patentable subject matter.

Claim 23 recites a method where, once a “generic” peripheral receives executable code and executes the code, the peripheral transmits a signal to a gaming device controller by which the peripheral identifies itself. Acres does not teach or suggest a configuration where peripherals are associated with a gaming device in a generic format, and only after executable code is provided does the device configure itself and identify itself as a particular known peripheral type or device.

Dependent Claims 26-30

Claims 26-30 are believed allowable for at least the reason they depend from allowable independent Claim 25.

New Claims 31-36

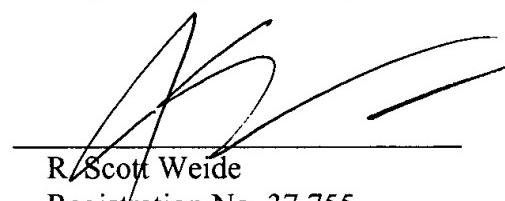
New Claims 31-36 are believed allowable for like reasons detailed above. As indicated, Acres does not teach or suggest providing control code to a peripheral device of a gaming machine, providing such code in response to a signal, or generating such a signal in response to a resetting of the peripheral device.

**Appl. No.** : 09/823,833  
**Filed** : March 30, 2001

Summary

Applicants assert that Claims 1-4 and 6-36 are in a condition for allowance and respectfully request a notice as to the same. If any matters remain outstanding, the Examiner is invited to contact the undersigned by telephone.

Respectfully submitted,

Dated: October 17, 2002 By:   
R. Scott Weide  
Registration No. 37,755  
Weide & Miller, Ltd.  
11<sup>th</sup> Floor, Suite 1130  
330 South 3<sup>rd</sup> Street  
Las Vegas, NV 89101  
(702)-382-4804 (Pacific time)

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicant : LeMay, et al. ) Group Art Unit: 3713

Appl. No. : 09/823,833 )

Filed : March 30, 2001 )

For : **METHOD AND APPARATUS  
FOR DOWNLOADING  
PERIPHERAL CODE** )

Examiner : Aaron L. Enatsky )

I hereby certify that this correspondence and all  
marked attachments are being deposited with the  
United States Postal Service as first-class mail in  
an envelope addressed to: Assistant  
Commissioner for Patents, Washington, D.C.  
20231, on

October 14, 2002

(Date)  
R. Scott Weide, Reg. No. 37,755

**ADDENDUM TO RESPONSE TO OFFICE ACTION**

Assistant Commissioner for Patents  
Washington, D.C. 20231

Dear Sir:

This is an Addendum to the Response to Office Action showing the changes made to the specification/claims made thereby.

**IN THE SPECIFICATION:**

Please replace the paragraph appearing at page 4, lines 13-16 with the following:

In one embodiment, peripheral control or operational code is stored at a data mass storage device associated with the game control device. In another embodiment, the control or operations code is transmitted from a remote location, such as a remote or central server, over a communications link to the [said] game control device to the peripheral.

**Appl. No.** : 09/823,833  
**Filed** : March 20, 2001

Please replace the paragraph appearing at page 18, line 17 to page 19, line 6 with the following:

In one embodiment, once peripheral control code has been downloaded to the peripheral 40, the code is provided to the peripheral a second time. The peripheral 40 utilizes this second copy of the code in a verification procedure, comparing the stored first copy to the newly transmitted second copy. If differences are found between the two versions of the code, then the version of the code which was downloaded and stored is not deemed authentic. The controller 54 of the peripheral 40 may then be arranged to request a new, third copy of the code for download and storage in replacement of the code which is currently stored, and verification procedure may repeat. In this embodiment, the second copy of the code is not stored permanently at the peripheral 40, but is only used in a comparison procedure. As is well known, this comparison procedure may comprise a bit-for-bit comparison or other method of verification now known or later developed. Of course, in this embodiment, the controller 54 of the peripheral 40 is provided with code arranged to cause the peripheral 40 to re-request the code after it has been stored, and to utilize this second requested copy of the code in the verification process.

Please replace the paragraph appearing at page 23, line 19 to page 24, line 3 with the following:

Figure 6 illustrates an operation flow diagram of an example method of creating the authentication file. This method is one exemplary method of operation and it is contemplated that other methods of creating authentication data may be utilized. Further, this method is available for

**Appl. No.** : 09/823,833  
**Filed** : March 20, 2001

use on any of a removable media, fixed or mass media, software stored on a network, or [other] any other data storage apparatus. For example, the method is available for authenticating peripheral code which is stored on a removable CD-ROM associated with the master gaming controller 42. The method is also available for authenticating peripheral code which is stored at the mass storage device 46 of the master gaming controller 42.

Please replace the paragraph appearing at page 24, lines 11-20 with the following:

At a step S150 the authentication data creation process loads software application files, such as the peripheral control code or video/audio peripheral operational data to a removable media. In other methods, the software may comprise files other than application files and the files may be loaded on the media prior to the initiation of [the] this process. Next, at a step S152, the operation creates a shell file that will become the authentication file storing the FVT.

Please replace the paragraph appearing at page 24, line 22 to page 25, line 11 with the following:

Thereafter, at a step S158, the operation stores the hash value in the FVT. In one preferred embodiment the hash value is stored with an association with the application file from which the hash value was created. Next, at a decision step S160, the operation determines if there are additional files on the media to execute the hash operation. If there are files for which a hash value has not been created, then the operation returns to step S154 and the operation repeats. If at decision step S160 the operation determines that no additional files exist on which to perform the hash

**Appl. No.** : 09/823,833  
**Filed** : March 20, 2001

operation, then the operation progresses to a step S162 and the method executes the hash operation on all hash values presently stored in the FVT. The hash operation creates a unique hash value for the hash values stored in the FVT to provide means to detect tampering or unwanted alteration of the hash values in the FVT. This hash value generated by executing the hash operation on the stored hash values is referred to herein as a content signature of the hash values. Next, at a step S164, the operation encrypts the content signature, [and] stores it in the FVT; then, the operation hashes the entire FVT file and obtains a signature for the entire FVT file. [Next, at a step S164, the operation hashes the entire FVT file and obtains a signature for the entire FVT file.]

Please replace the paragraph appearing at page 27, lines 12-23 with the following:

Next, at a step S356, the operation searches the media for the verification file stored on the media. The creation and content of the verification file is discussed above. At a step S358, the operation utilizes the decryption algorithms from the secure memory to decrypt the file signature stored in the FVT . The encrypted file signature is shown as element [5386] S286 on Figure 7. After decrypting the file signature value stored in the FVT, the operation performs a hash operation on the FVT file up to the encrypted content signature [5284] S284 (see Figure 7), to obtain a re-calculated file signature. This occurs at a step S360. Thereafter, at a step S362, the operation compares the decrypted signature to the re-calculate file signature to check for differences in the values. At a decision step S364, a determination is made whether the signatures match. If the decrypted signature does not match the re-calculated signature, the operation progresses to a step S366 and the process terminates. Such a failure to match at step S364 indicates possible tampering

**Appl. No.** : 09/823,833  
**Filed** : March 20, 2001

or alteration and the installation or game operation should not occur or may have occurred inaccurately.

Please replace the paragraph appearing at page 28, line 20 to page 29, line 2 with the following:

At a step S384, the operation compares the hash value from the FVT to the re-calculated hash value for the corresponding software file stored on the media. At a decision step S386 a determination is made as to whether these two hash values match. If the values do not match, the operation moves to a step S388 and the process terminates. If the values match, the operation moves to a decision step [S390] (not shown) wherein the operation determines if all the entries of the FVT have been compared to re-calculated values.

Please replace the paragraph appearing at page 29, lines 4-12 with the following:

If at the decision step [S390] there are additional FVT entries to compare, the operation returns to step S380 and the operation repeats as shown. If at the decision step [S390] all the FVT entries have been compared to re-calculated entries, the operation progress to a step [S392] wherein the determination is made that the media (such as peripheral control code files) has been authenticated. It is contemplated that this process can occur on any media (including control code files, operational data such as audio/video data) for which authentication is desired. It is further contemplated that many other variations may be made to the general process outlined herein without

**Appl. No.** : 09/823,833  
**Filed** : March 20, 2001

departing in scope of authentication to determine that the software control code on the media, fixed, removable, or otherwise, is trustworthy.

**IN THE CLAIMS:**

1. A method of operating a gaming device including a game device controller and at least one peripheral having a peripheral controller associated with said game device controller comprising the steps of:

initiating operation of said gaming device;

transmitting a signal from said peripheral device to said game device controller causing said game device controller to provide control code to said peripheral device;

[authenticating said control code;]

transmitting said control code to said peripheral device;

authenticating said control code transmitted to said peripheral device at said peripheral device;

storing said control code at said programmable memory of said peripheral device; and executing said control code with said peripheral controller for effecting operation of said peripheral device.

2. The method in accordance with Claim 1 wherein said initiating step comprises providing power to said gaming device peripheral and said step of transmitting said signal is performed in response to said step of providing power.

**Appl. No.** : 09/823,833  
**Filed** : March 20, 2001

3. The method in accordance with Claim 1 wherein said initiating step comprises resetting said peripheral device and said step of transmitting said signal is performed in response to said resetting.

6. The method in accordance with Claim 1 [5] further including the steps of shutting off power to said peripheral device, [of] removing data from said programmable memory in response to said power being shut off to said peripheral device, and then providing power to said gaming device and said peripheral device to initiate operation of said gaming device and peripheral device.

9. In a gaming device, a method for providing control code for operation of a peripheral device associated with a gaming device controller comprising the steps of:

providing a peripheral controller adapted to control said peripheral device and a programmable memory associated with said controller;

providing a signal by said peripheral device for causing control code to be transmitted from a remote location to said peripheral;

transmitting said control code to said peripheral;

storing said control code at said programmable memory; and

executing said code with said peripheral controller to enable the operation of said peripheral device by said peripheral controller.